Amendments to the Specification

Please amend the paragraphs numbered below as shown:

[62] In an IBE scheme adapted to implement a CBE scheme, the authorizer generates a recipient "decryption key" using a key generation secret that is a secret of the authorizer. The decryption key forms a public key/ private pair with a recipient "encryption" key. In one embodiment, the recipient ~~recipient~~ decryption key is a signature on the recipient encryption key generated using the [[the]] key generation secret. The message sender encrypts a digital message using the recipient public key and the recipient encryption key to create an encrypted digital message. The recipient decrypts the encrypted digital message using the recipient private key and the recipient decryption key. Since the sender encrypts the message using both the recipient public key and the recipient encryption key, the recipient needs both the recipient private key and recipient decryption key to decrypt the encrypted message. Because both keys are required, the recipient decryption key need not be kept secret. For example, since the recipient decryption key is in fact a signature by one or more authorizers, the decryption can be treated as a signature; it can be used as verifiable proof that the recipient has received appropriate authorization.

[63] In general, the encryption key can correspond to a document D and the decryption key to the signature s_D, the authorizer's signature on the document D using s, the authorizer's key-generation secret. If the decryption key, and hence the encryption key, are updated using a schedule known to the message sender, the sender can encrypt a message that the recipient can decrypt only when the recipient ~~recieves~~ receives a decryption key corresponding to the encryption key used to encrypt the message.

[87] Secure and practical HIDE schemes are described in a co-pending patent application ~~(attorney reference number 10745/107)~~ no. 10/384,328, the contents of which are incorporated herein for all purposes by this reference.